OWASP, PT.OWASP , IBWAS'10 & Cia.

WTF is this? Do I need that? Why should I give a sh*t?

PT.OWASP

www.owasp.org
www.owasp.org/index.php/Portuguese

Carlos Serrão

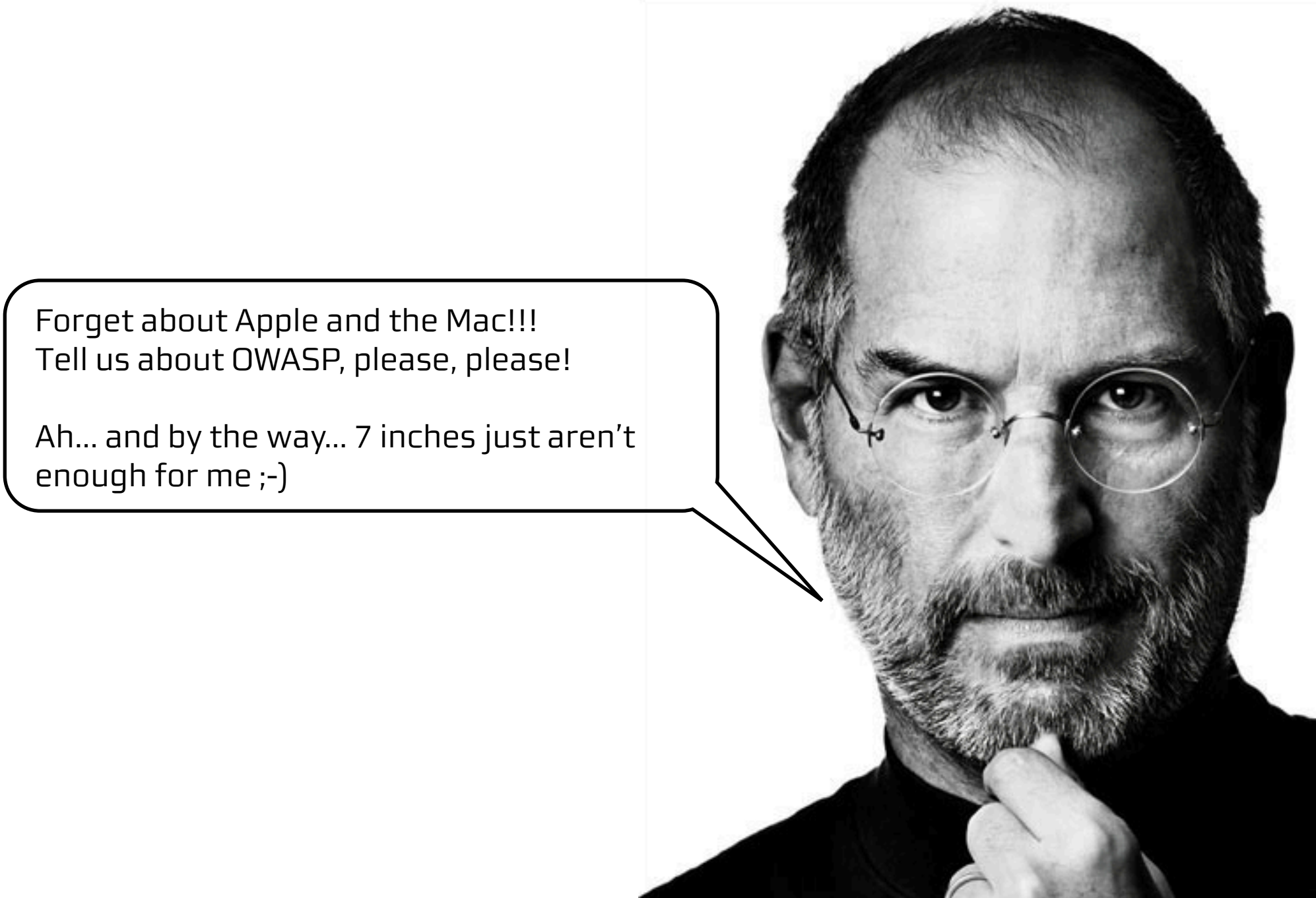
carlos.serrao@iscte.pt
carlos.j.serrao@gmail.com

http://www.carlosserrao.net
http://blog.carlosserrao.net
http://www.linkedin.com/in/carlosserrao

OWASP
The Open Web Application Security Project

... countdown to

Back to the Mac.


Forget about Apple and the Mac!!!
Tell us about OWASP, please, please!
Ah... and by the way... 7 inches just aren't enough for me ;-)

OWASP?

- ... mas primeiro...

About me (eu, je, ich, jag, 我)

- Assistant Professor at ISCTE-IUL (Lisbon University Institute)/SoTA (School of Technology and Architecture)/DCTI
- ADETTI-IUL Researcher and Project Manager
- Projects. EC, National, Private projects.
- OWASP.PT leader?!?!?
- Author. Papers. Books.
- Geek. Love technology. Huge fan of gadgets.
- OS agnostic. Linux, Mac OS X, Windows. Bring them all!!!

OWASP?

- Open Web Application Security Project
  - Promove o desenvolvimento seguro de software
  - Orientado para o desenvolvimento de serviços baseados na web
  - Focado principalmente em aspectos de desenvolvimento do que em web-design
  - Um fórum aberto para discussão
  - Um recurso gratuito e livre para qualquer equipa de desenvolvimento

OWASP?

- Open Web Application Security Project
  - *an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted*
  - Promover o desenvolvimento seguro
  - Auxiliar a tomada de decisão quanto ao risco
  - Oferecer recursos gratuitos
  - Promover a contribuição e partilha de informação

OWASP?

- Open Web Application Security Project
  - Organização sem fins lucrativos, orientada para esforço voluntário
    - Todos os membros são voluntários
    - Todo o trabalho é “doado” por patrocinadores
  - Oferecer recursos livres para a comunidade
    - Publicações, Artigos, Normas
    - Software de Testes e de Formação
    - Chapters Locais & Mailing Lists
  - Suportada através de patrocínios
    - Suporte de empresas através de patrocínios financeiros ou de projectos
    - Patrocínios pessoais por parte dos membros

OWASP?

- O que oferece?
  - Publicações
    - OWASP Top 10
    - OWASP Guide to Building Secure Web Applications
  - Software
    - WebGoat
    - WebScarab
    - oLabs Projects
    - .NET Projects
  - Chapters Locais
    - Orientação das comunidades locais

OWASP?

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing

Automated Security Verification

- Penetration Testing Tools
- Code Review Tools

Manual Security Verification

- ESAPI

Security Architecture

- AppSec Libraries
- ESAPI Reference Implementation
- Guards and Filters

Secure Coding

- Reporting Tools

AppSec Management

- Flawed Apps
- Learning Environments
- Live CD
- SiteGenerator

AppSec Education

OWASP?

- Top 10 Web Application Security Risks/ Vulnerabilities
  - Uma lista dos 10 aspectos de segurança mais críticos
  - Actualizado numa base anual
  - Crescente aceitação pela indústria
    - Federal Trade Commission (US Gov)
    - US Defense Information Systems Agency
    - VISA (Cardholder Information Security Program)

- Está a ser adoptado como um standard de segurança para aplicações web

OWASP?

http://www.owasp.org/index.php/Top_10

OWASP?

- Guia para o Desenvolvimento Seguro de Web Apps
  - Oferece um conjunto de linhas gerais para o desenvolvimento de software seguro
    - Introdução à segurança em geral
    - Introdução à segurança aplicacional
    - Discute áreas-chave de implementação
      - Arquitectura
      - Autenticação
      - Gestão de Sessões
      - Controlo de Acesso e Autorização
      - Registo de Eventos
      - Validação de Dados
  - Em contínuo desenvolvimento

OWASP?

- WebGoat
  - Essencialmente é uma aplicação de treino
  - Oferece
    - Uma ferramenta educacional usada para ensinar e aprender sobre segurança aplicacional
    - Uma ferramenta para testar ferramentas de segurança
  - O que é?
    - Uma aplicação web J2EE disposta em diversas “Lições de Segurança”
    - Baseado no Tomcat e no JDK 1.5
  - Orientada para o ensino
    - Fácil de usar
    - Ilustra cenários credíveis
    - Ensina ataques realistas e soluções viáveis

OWASP?

- WebScarab
  - Uma framework para analisar tráfego HTTP/HTTPS
  - Escrito em Java
  - Múltiplas utilizações
    - Programador: fazer o debug das trocas entre o cliente e servidor
    - Analista de Segurança: analisa o tráfego e identifica vulnerabilidades
  - Ferramenta técnica
    - Focada em programadores de software
    - Arquitectura extensível de plug-ins
    - Open source; de fácil expansão
    - Poderosa
  - Obter a ferramenta
    - http://www.owasp.org/software/webscarab.html

Delegações OWASP

- Desenvolvimento de comunidades
  - As delegações locais proporcionam oportunidades para os membros OWASP poderem partilhar ideias e aprender mais sobre segurança da informação
  - Aberto a *TODOS*
  - Oferecer um fórum para discussão de assuntos em contextos locais/regionais
  - Oferecer o local para convidados poderem apresentar novas ideias e projectos


Greenland
Iceland
Suomi
Finland
Sverige
Norge
Россия
Russia
Canada
United States
México
North Atlantic Ocean
Polska
Україна
Ukraine
Kazakhstan
Mongolia
France
Italia
Italy
España
Spain
Türkiye
Turkey
Iraq
Iran
Afghanistan
Saudi Arabia
China
Korea
Japan
India
Algeria
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
South Africa
Madagascar
Indian Ocean
Indonesia
Papua New Guinea
Australia
New Zealand
Venezuela
Colombia
Perú
Brasil
Brazil
Bolivia
Chile
Argentina
South Atlantic Ocean
POWERED BY Google
Map data ©2009 Europa Technologies - Terms of Use

Delegações OWASP

- O que oferecem?
  - Reuniões (regulares)
  - Mailing Lists
  - Apresentações e Grupos
  - Ambientes independentes do vendedor
  - Fóruns de discussão aberta

PT.OWASP

- ... alguns dados

- Membros (ML)
  - 71 membros
- Web-site
  - http://www.owasp.org/index.php/Portuguese
- Mailling-List
  - owasp-portuguese@lists.owasp.org

PT.OWASP

- Participação em alguns dos projectos activos do OWASP (documentação e ferramentas)
- Propor o lançamento de novos projectos
- Promover a discussão de ideias na nossa lista de correio electrónico
- Dinamizar a participação nas nossas reuniões
- Organização de conferências
- Promover e oferecer suporte à comunidade OWASP em geral, em particular a comunidade portuguesa

PT.OWASP

- Objectivos:
  - Manter um calendário de reuniões periódicas
    - Realista: 1 reunião/evento a cada 3 ou 4 meses
  - Promover a missão da OWASP
  - Promover os projectos, ferramentas e documentação da OWASP
  - Promover a troca e disseminação livre de informação sobre segurança de informação e segurança de aplicações e sistemas web-based
  - Promover o lançamento de novas ideias e de novos projectos
  - Envolver os membros em projectos on-going

PT.OWASP

- A participação nas reuniões da OWASP Portugal é livre e gratuita
  - Modelo: aparece e traz um amigo (e ideias para partilhar)

- Apresentação sobre um tema
- Discussão de uma ideia
- Debate de problemas
- Lançar iniciativas
- Planear actividades

PT.OWASP

- Reuniões periódicas
- Blog/Site oficial da OWASP@PT
  - http://www.owasp.org/index.php/Portuguese
- Eventos de disseminação/formação
- Conferências
- Projectos de tradução de documentação e ferramentas (em conjunto com OWASP Brasil)
- Lançamento de novos projectos
- Estreitar relações com OWASP Espanha

História e Actividade

- 2007
  - Nasce o chapter português
  - Actividade quase nula
- 2008
  - OWASP EU Summit 08
  - Albufeira, Algarve, Portugal
- 2009
  - owasp@IPCB (Castelo Branco), owasp@IPViseu (Viseu), owasp@UBI (Covilhã)
  - IBWAS'09, Madrid
- 2010
  - owasp@ISCTE-IUL
  - Samy Kamkar, How I met Your Girlfriend, Lisboa
  - IBWAS'10, Lisboa
- 2011
  - ????

OWASP EU SUMMIT 2008

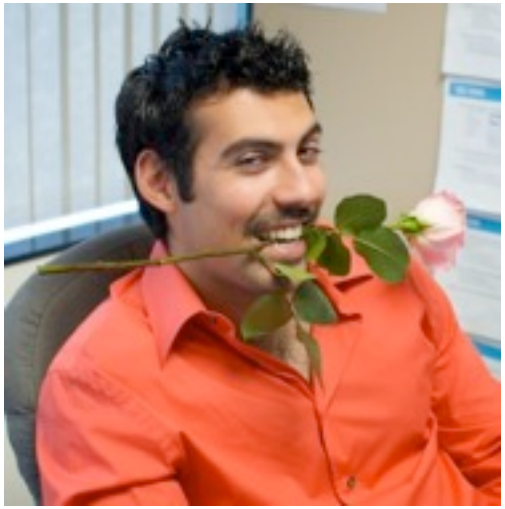
- O *maior* evento OWASP de sempre
  - 1 semana, +100 pessoas (de todo o Mundo)
  - Apresentação de Projectos
  - Sessões de Trabalho
  - Formação
  - + 1 dia de Demo na UAlg

IBWAS'09

- 1st. OWASP Iberic Web App Sec 2009
- Dezembro 2009
  - Universidade Politécnica de Madrid
  - Speakers, entre os quais Bruce Schneier

Samy Kamkar - Lisboa

- Sobre
  - http://samy.pl
  - @samykamkar
  - desenvolveu 1º worm XSS para o MySpace
    - 1M utilizadores infectados < 24h
  - co-fundador da Fonality, Inc.
    - produtos de IP PBX



"think bad, do good"

- How I met Your Girlfriend
  - BlackHat 2010 - LV, USA
  - conjunto de novos ataques descobertos, executados através da Web, com o objectivo de conhecer a vossa namorada ;-)
- Integrado numa Tour Europeia patrocinada pela OWASP

IBWAS'10

- 2nd. OWASP Ibero-American Web App Sec 2010
- Novembro 2010
  - ISCTE-IUL
    - 25, 26 | Conferência
      - Sessões Técnicas/Profissionais
      - Sessões de Research/Académicas
    - 27 | Sessões de Formação/Tutoriais
  - http://www.ibwas.com

IBWAS'10

- 25, 26 | Conferência
  - Sessões Técnicas/ Profissionais
    - keynotes e sessões curtas
  - Sessões de Research/ Académicas
    - papers, com avaliação de pares
- 27 | Sessões de Formação/ Tutoriais
  - 1 dia
  - 1/2 dia
  - em processo de escolha

IBWAS'10
2ND. OWASP IBERO-AMERICAN WEB APPLICATIONS SECURITY CONFERENCE

IBWAS'10


IB
WAS '10
2nd. OWASP Ibero-American Web Applications Security Conference

IBWAS'10

- Como participar:
  - propor uma sessão de treino/tutorial (deadline: expired)
    - http://www.owasp.org/index.php/IBWAS10#tab=Training
  - submeter uma comunicação (deadline: 31.Out.2010)
    - http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers
  - participar numa sessão de treino
    - http://www.owasp.org/index.php/IBWAS10#tab=24th_November_-_Tutorials
  - assistir à conferência
    - http://www.owasp.org/index.php/IBWAS10#tab=25th.2F26th_November_-_Conference
  - patrocinar
    - http://ibwas09.netmust.eu/files/IBWAS_sponsorship.pdf

IBWAS'10

- Sponsors
  - oportunidades de *sponsorship*
    - Diamond Sponsor
    - Platinum Sponsor
    - Gold Sponsor
    - Silver Sponsor
    - Lunch Sponsor
    - Cofee Break Sponsor
    - Badge, Lanyard
    - Notepad
    - Pen Sponsor
  - permitem tornar o evento progressivamente gratuito

ISCTE IUL
Instituto Universitário de Lisboa
Lisbon University Institute

adetti

MAXDATA

NOESIS
internet security auditors

LASIGE
FACULDADE · DE · CIÊNCIAS · UNIVERSIDADE · DE · LISBOA
Laboratório de Sistemas Informáticos de Grande Escala

Finalmente...

- ... juntem-se a nós.
- Participem!
  - Mailing List
  - Blog
  - Reuniões
  - Eventos
  - Projectos
  - Ideias
- Informação útil
  - http://www.owasp.org
  - http://www.owasp.org/index.php/Portuguese
  - http://webappsec.netmust.eu


That's all Folks!


meo

OWASP, PT.OWASP , IBWAS'10 & Cia.

WTF is this? Do I need that? Why should I give a sh*t?

PT.OWASP

www.owasp.org
www.owasp.org/index.php/Portuguese

Carlos Serrão

carlos.serrao@iscte.pt
carlos.j.serrao@gmail.com

http://www.carlosserrao.net
http://blog.carlosserrao.net
http://www.linkedin.com/in/carlosserrao

OWASP
The Open Web Application Security Project